

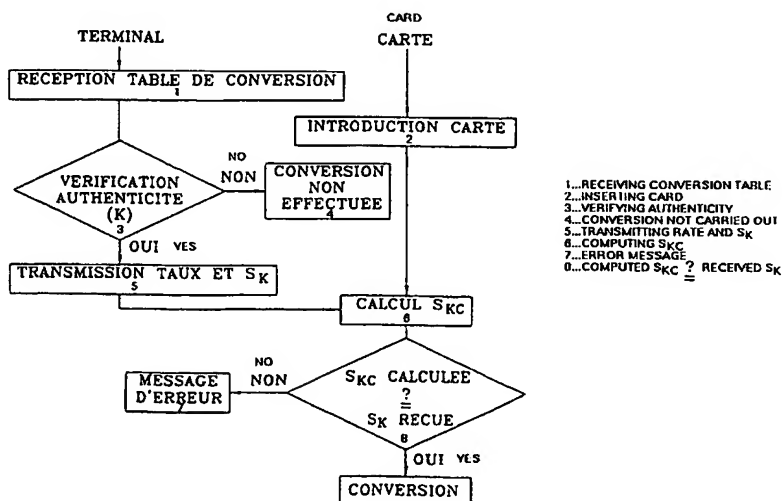


## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>7</sup> : <b>G07F 7/08</b>		A1	(11) Numéro de publication internationale: <b>WO 00/11621</b>
			(43) Date de publication internationale: 2 mars 2000 (02.03.00)
(21) Numéro de la demande internationale: PCT/FR99/02014		(81) Etats désignés: AU, CA, CN, JP, KR, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) Date de dépôt international: 19 août 1999 (19.08.99)			
(30) Données relatives à la priorité: 98/10569 20 août 1998 (20.08.98) FR		Publiée Avec rapport de recherche internationale.	
(71) Déposant (pour tous les Etats désignés sauf US): BULL CP8 [FR/FR]; 68, route de Versailles, Boîte postale 45, F-78430 Louveciennes (FR).			
(72) Inventeur; et (75) Inventeur/Déposant (US seulement): SALLES, Jean-Luc [FR/FR]; 105, rue du Château, F-92100 Boulogne Billancourt (FR).			
(74) Mandataire: CORLU, Bernard; Bull S.A., PC58F35, 68, route de Versailles, F-78434 Louveciennes Cedex (FR).			
(54) Title: PORTABLE OBJECT SUCH AS AN ELECTRONIC PURSE FOR PAYMENT IN DIFFERENT CURRENCIES AND ASSOCIATED PAYMENT PROTOCOL			
(54) Titre: OBJET PORTATIF DU TYPE PORTE-MONNAIE ELECTRONIQUE PERMETTANT LE PAIEMENT DANS DIFFERENTES DEVISES ET PROTOCOLE DE PAIEMENT ASSOCIE			

## (57) Abstract

The invention concerns a portable object comprising an electronic purse application, wherein said data-exchange protocol defines an instruction for operating electronic currency conversion. The method consists in: (a) storing in the portable object an electronic currency conversion table certified by an original electronic signature ( $S_K$ ) by a banking authority; (b) authenticating said conversion table, and, on the basis of said conversion table authentication, the currency conversion rate value constituting an authenticated conversion rate value; (c) carrying out the conversion of the electronic purse current balance, from said authenticated conversion rate value, to generate a converted current balance value, and storing the converted current balance value, or, in the absence of authentication, (d) stopping the current transaction and sending an error message.



(57) Abrégé

Dans un objet portatif comportant une application de porte-monnaie électronique, ce protocole d'échange de données définit une instruction d'opération de conversion de monnaie électronique. Il consiste à: (a) mémoriser dans l'objet portatif une table de conversion de monnaie électronique certifiée par une signature électronique d'origine (SK) par une autorité bancaire, la table de conversion comportant au moins une valeur de taux de conversion; (b) authentifier ladite table de conversion, et, sur authentification de ladite table de conversion, la valeur de taux de conversion constituant une valeur de taux de conversion authentifiée, (c) procéder à la conversion du solde courant du porte-monnaie électronique, à partir de ladite valeur de taux de conversion authentifiée, pour engendrer une valeur du solde courant convertie, et mémoriser la valeur du solde courant convertie, ou, en l'absence d'authentification, (d) bloquer la transaction courante et émettre un message d'erreur.

**UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroon	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

Titre :

OBJET PORTATIF DU TYPE PORTE-MONNAIE ELECTRONIQUE  
PERMETTANT LE PAIEMENT DANS DIFFERENTES DEVICES ET  
PROTOCOLE DE PAIEMENT ASSOCIE

5

La présente invention se rapporte à un objet portatif, notamment une carte porte-monnaie électronique permettant le paiement dans différentes devises et à un protocole de paiement associé.

10

A l'heure actuelle, les cartes à microprocesseur sont utilisées dans le domaine bancaire pour effectuer des transactions. Une carte bancaire est liée au compte bancaire de son porteur. Elle permet au commerçant de s'assurer que le porteur est bien titulaire d'un compte bancaire et, par l'enregistrement de la transaction dans le microprocesseur de la carte, que la transaction est bien débitée du compte du porteur. Ainsi, la carte bancaire ne contient pas d'argent. Elle se borne à mémoriser des débits qui seront effectués ultérieurement dans le compte bancaire du porteur.

20

Une carte porte-monnaie électronique, désignée dans la suite par l'abréviation PME, fonctionne différemment. Le principe d'utilisation d'une carte PME est tout à fait comparable à celui d'un porte-monnaie traditionnel contenant de l'argent sous forme de billets et/ou de pièces de monnaie, à la différence qu'une carte PME manipule de l'argent électronique. On charge initialement la carte PME avec une certaine somme d'argent, qui diminue au fur et à mesure des transactions. Lorsque la somme est nulle, toute transaction est impossible. A tout moment, le porteur peut prendre connaissance du solde de sa carte en l'introduisant dans un lecteur et en effectuant une interrogation.

25

30

La somme d'argent contenue dans la carte PME est exprimée dans une devise déterminée, qui correspond par

exemple au pays d'utilisation dont le porteur de la carte est le ressortissant. Un problème se pose donc lorsque le porteur souhaite effectuer une transaction dans une devise différente de celle utilisée habituellement par la carte, au cours d'un déplacement à l'étranger par exemple.

Le type de devise est généralement écrit dans une mémoire programmable non volatile de la carte. La lecture de cette donnée est libre mais son écriture est subordonnée à des droits d'accès.

Une solution connue pour changer la devise d'une carte PME, et convertir le solde de cette dernière dans une nouvelle devise, consiste à introduire et connecter la carte à un terminal bancaire, puis à effectuer une transaction consistant en un débit d'un montant égal au solde courant de la carte. Cette opération a pour objet de vider la carte. Puis le terminal modifie dans la carte la donnée représentative de la devise et convertit dans la nouvelle devise l'argent électronique reçu. Ensuite, le terminal, par une opération de crédit, recharge la carte avec la même somme d'argent convertie dans la nouvelle devise.

Cette solution est contraignante car elle nécessite la réalisation de deux transactions successives, à savoir, un débit puis un crédit. De plus, du point de vue de la sécurité, elle présente un risque, par exemple en cas d'arrachement de la carte entre l'opération de débit et l'opération de crédit, le solde étant dans ce cas réduit à zéro de manière non justifiée. En outre, la solution connue manque de souplesse, car elle oblige le porteur de la carte ayant effectué une transaction consistant en un débit dans la devise courante de la carte, afin de vider cette carte, à se rendre dans une banque pour faire effectuer une transaction consistant en un crédit du même montant dans une autre devise, afin de recharger la carte.

La présente invention a pour but de pallier les inconvénients précités.

La présente invention a notamment pour but de créer une nouvelle instruction dans une carte PME, de créer un nouveau protocole de communication entre une carte PME et un terminal de transaction, et de sécuriser les cartes PME et les terminaux de transaction vis-à-vis des risques de création frauduleuse de monnaie électronique, la fraude pouvant consister, soit à effectuer successivement deux conversions inverses sur deux terminaux ayant des tables de conversion élaborées à des dates différentes, soit à effectuer successivement un grand nombre de conversions sur une pluralité de terminaux différents.

Dans ce but, la présente invention propose, dans un objet portatif comportant au moins une application de porte-monnaie électronique, cet objet portatif comprenant des moyens de traitement de l'information et au moins une mémoire programmable non volatile, comportant une zone de mémorisation de transactions relatives à l'application de porte-monnaie électronique, ces transactions comportant au moins une instruction d'opération de débit et une instruction d'opération de crédit, un protocole d'échange de données définissant une instruction d'opération de conversion de monnaie électronique d'une devise de départ en une devise courante, consistant au moins à :

- (a) mémoriser dans ledit objet portatif une table de conversion de monnaie électronique certifiée par au moins une signature électronique d'origine par une autorité bancaire, ladite table de conversion de monnaie électronique comportant au moins une valeur de taux de conversion d'une devise de départ en au moins une devise courante ;

(b) authentifier ladite table de conversion de monnaie électronique, par vérification de ladite signature électronique d'origine, et, en cas d'authentification de ladite table de conversion de monnaie électronique, la valeur de taux de conversion constituant une valeur de taux de conversion authentifiée,

(c) procéder à la conversion d'un solde courant du porte-monnaie électronique, à partir de ladite valeur de taux de conversion authentifiée, pour engendrer une valeur du solde courant convertie, et mémoriser la valeur du solde courant convertie dans ladite mémoire non volatile, ou, en l'absence d'authentification,

(d) bloquer une transaction courante.

L'invention concerne aussi un protocole de communication entre un objet portatif utilisant une première devise habituelle prédéterminée et un terminal de transaction utilisant une deuxième devise habituelle prédéterminée, ledit objet portatif comportant au moins une application de porte-monnaie électronique, et comprenant des moyens de traitement de l'information et au moins une mémoire programmable non volatile comportant une zone de mémorisation de transactions relatives à l'application de porte-monnaie électronique, ces transactions comportant au moins une instruction d'opération de débit et une instruction d'opération de crédit, ledit protocole de communication comprenant des étapes suivant lesquelles :

(a) le terminal reçoit en provenance d'une autorité bancaire une table de conversion de monnaie électronique ;

(b) on introduit dans le terminal ledit objet portatif afin de réaliser une transaction ;

- 5 (c) le terminal transmet à l'objet portatif le  
taux de conversion de ladite première devise  
dans ladite deuxième devise, contenu dans  
ladite table de conversion de monnaie  
électronique, accompagné d'une signature  
électronique d'origine relative audit taux,  
ladite signature électronique d'origine  
étant calculée à l'aide d'une clé  
prédéterminée ;
- 10 (d) l'objet portatif vérifie ladite signature  
électronique d'origine à l'aide de ladite  
clé, préalablement mémorisée dans l'objet  
portatif ou d'une clé corrélée à celle-ci ;
- 15 (e) si la signature électronique d'origine est  
vérifiée, l'objet portatif effectue la  
conversion du solde courant mémorisé de  
ladite première devise dans ladite deuxième  
devise au moyen dudit taux de conversion et  
mémorise le solde courant converti ;
- 20 (f) l'objet portatif effectue ladite transaction.

L'invention concerne encore un objet portatif  
comprenant des moyens de traitement de l'information et des  
moyens de mémorisation de l'information, caractérisé en ce  
25 qu'il inclut :

- 30 - des moyens pour stocker de façon provisoire dans les  
moyens de mémorisation une table de conversion de  
monnaie électronique reçue de l'extérieur de l'objet  
portatif et comportant au moins une valeur de taux de  
conversion d'une devise de départ en au moins une devise  
courante, ainsi qu'une signature électronique d'origine  
( $S_K$ ) de cette table de conversion, calculée au moyen  
d'un algorithme de signature et d'une clé de signature  
35 déterminés ;

- des moyens pour authentifier ladite table de conversion en vérifiant ladite signature électronique d'origine ( $S_K$ ) de la table de conversion reçue, au moyen d'un algorithme de vérification de signature et d'une clé de vérification de signature déterminés ;
- des moyens pour stocker de façon durable, en cas d'authentification positive, la table de conversion dans les moyens de mémorisation ; et
- des moyens pour calculer une valeur de solde courant convertie à partir d'une valeur de solde courant et d'une valeur de taux de conversion extraite de la table de conversion authentifiée.

D'autres particularités et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui suit de modes particuliers de réalisation de l'invention, donnés à titre d'exemples non limitatifs. La description se réfère aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 est une représentation schématique d'une carte à microprocesseur ayant une fonctionnalité de conversion conforme à la présente invention, dans un mode particulier de réalisation ;

- la figure 2 est un organigramme illustrant la succession des étapes définissant la nouvelle instruction de conversion dans la carte PME ;

- la figure 3 est une représentation schématique des divers éléments constitutifs d'un message contenant une valeur de taux de conversion transmis par le terminal à la carte ;

- la figure 4 est une représentation schématique de la zone de mémorisation de transactions comprise dans la carte PME ;

- les figures 5A et 5C sont des organigrammes illustrant la succession des étapes du protocole de



communication de la présente invention, respectivement dans un mode particulier de réalisation où le terminal ne comporte pas de module de sécurité et dans un mode particulier de réalisation où le terminal comporte un module de sécurité ;

- la figure 5B représente de façon schématique un terminal doté d'un module de sécurité ;

- la figure 6 est un organigramme illustrant le fonctionnement du compteur de conversions ;

- la figure 7 est un organigramme illustrant la comparaison de la date d'élaboration de la table de conversion à une date courante de référence reçue par voie hertzienne ; et

- la figure 8 est un schéma illustrant la comparaison entre la date d'élaboration d'une table de conversion et la date de la dernière transaction mémorisée dans la carte.

Comme le montre la figure 1, on considère une carte à microprocesseur 10 qui comporte au moins une application de porte-monnaie électronique. La carte 10 comprend un module d'entrée-sortie 12 permettant à la carte 10 de communiquer avec l'extérieur, et notamment avec un terminal de transaction dépendant d'une autorité bancaire. Les opérations effectuées par la carte sont commandées par un microprocesseur 14, relié au module d'entrée-sortie 12.

La carte 10 comporte également un système d'exploitation, implanté dans une mémoire morte 16 du type ROM. La mémoire morte 16 est reliée au microprocesseur 14.

La carte 10 comporte en outre une mémoire programmable non volatile 18, du type EPROM ou EEPROM ou encore FERAM. La mémoire programmable non volatile 18 est reliée à la mémoire morte 16 et au microprocesseur 14. Elle comporte une zone de mémorisation de transactions relatives à l'application de porte-monnaie électronique et une zone

système, comportant par exemple un numéro d'identification de la carte 10. Ces transactions sont des instructions pour effectuer soit des opérations de débit, soit des opérations de crédit.

5           La zone de mémorisation de transactions, qui contient un nombre limité N d'emplacements, est avantageusement cyclique, comme illustré par la figure 4, c'est-à-dire qu'un pointeur indique successivement l'adresse des emplacements pour mémoriser chaque  
10 transaction, qui consiste soit en une opération de crédit CR, soit en une opération de débit DE, soit en une opération de conversion CO. Lorsque les N emplacements sont occupés, le pointeur indique à nouveau l'adresse du premier emplacement, dont le contenu est effacé et remplacé par la  
15 (N+1)<sup>ème</sup> transaction, et ainsi de suite.

L'ensemble constitué par le microprocesseur 14, la mémoire morte 16 et la mémoire programmable non volatile 18 peut être réalisé sous forme d'un microcontrôleur.

20           La carte 10 comprend en outre un module 20 de calcul de la signature électronique de données, dont le fonctionnement est décrit plus loin. Sur la figure 1, le module 20 a été représenté en tirets pour illustrer le fait qu'il peut être, soit de nature matérielle, soit de nature  
25 logicielle. Dans le second cas, il consiste en un programme stocké dans la mémoire ROM 16 et exécuté par le microprocesseur 14.

30           Le module d'entrée-sortie 12, le microcontrôleur, dont la ROM 16, et le module 20 de calcul de signature forment un circuit intégré, qui peut être réalisé sous forme d'un ASIC (Application Specific Integrated Circuit).

En tant que microprocesseur ou "puce", on pourra notamment utiliser un microprocesseur autoprogrammable à mémoire non volatile, tel que décrit dans le brevet américain n° 4 382 279 au nom de la demanderesse. Comme

indiqué en colonne 1, lignes 13-25 de ce brevet, le caractère autoprogrammable de la puce correspond à la possibilité pour un programme fi situé dans une mémoire ROM, de modifier un autre programme fj situé dans une mémoire programmable en un programme gj. Dans une variante, le microprocesseur de la puce est remplacé — ou tout du moins complété — par des circuits logiques implantés dans une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Comme indiqué ci-dessus, ils peuvent notamment être de type ASIC. A titre d'exemple d'ASIC, on peut citer le composant de la société SIEMENS commercialisé sous la référence SLE 4436 et celui de la société SGS-THOMSON commercialisé sous la référence ST 1335. Avantageusement, la puce sera conçue sous forme monolithique.

Conformément à la présente invention, on définit dans la carte à microprocesseur 10 une nouvelle fonctionnalité sous forme d'une nouvelle instruction de conversion CO, qui lui permet d'effectuer en une opération unique une conversion d'une devise de départ en une devise courante, ce qui augmente la rapidité de traitement, apporte davantage de sécurité et permet une harmonisation des opérations de change.

Pour cela, le terminal bancaire de transaction possède les valeurs de taux de conversion entre les devises et les transmet à la carte à l'occasion d'une transaction, sous forme de messages contenant chacun un identifiant de la devise, une valeur de taux de conversion, une date de mise à jour de la valeur de taux, et une signature électronique relative à la valeur de taux, comme illustré par la figure 3. La carte calcule alors son solde dans la nouvelle devise.

Les valeurs des taux de conversion sont transmises au terminal par une autorité bancaire, sous forme d'une table de données, dite table de conversion.

5 Le protocole d'échange de données qui définit une instruction d'opération de conversion de monnaie électronique d'une devise de départ en une devise courante est illustré par la figure 2.

10 Ce protocole consiste tout d'abord à mémoriser dans la carte une table de conversion de monnaie électronique. Cette table est certifiée par une autorité bancaire, au moyen d'une ou plusieurs signature(s) électronique(s) d'origine  $S_K$ . Cette table contient au moins la valeur de taux de conversion de la devise de départ en la devise courante.

15 Ces signatures électroniques sont établies au moyen d'un algorithme cryptographique déterminé, par exemple du type RSA (des inventeurs Rivest, Shamir et Adleman) ou DES (de l'anglais Data Encryption Standard), d'une clé fournie par l'autorité bancaire et de données. Ici, la signature est le résultat du calcul effectué à partir des données d'entrée constituées par la table de conversion.

20 L'étape suivante consiste, pour la carte, à authentifier la table de conversion. Pour cela, la carte calcule une signature électronique de contrôle  $S_{KC}$  relative à la valeur de taux de conversion de la devise de départ en la devise courante. Puis la carte compare la signature de contrôle  $S_{KC}$  à la signature d'origine  $S_K$ . Si ces signatures sont égales, la valeur de taux de conversion est authentifiée et la carte procède alors à la conversion de son solde courant, en multipliant ce solde par la valeur de  
25 taux de conversion reçue, puis mémorise la valeur du solde converti dans la mémoire programmable non volatile 18. Si  
30 les signatures d'origine  $S_K$  et de contrôle  $S_{KC}$  sont différentes, la carte bloque la transaction, un message

d'erreur est émis, et les données de taux de conversion sont détruites.

Selon un premier mode de réalisation, la table de conversion contient un identifiant pour chaque devise et la valeur du taux de conversion de chaque devise dans une devise de référence, telle que l'euro, ou la devise du pays où est installé le terminal, à titre d'exemples non limitatifs. Les valeurs des taux de conversion étant susceptibles de fluctuer, elles sont accompagnées d'une date de mise à jour. En outre, chaque couple de valeur de taux et date de mise à jour est signé par l'autorité bancaire, qui transmet également cette signature électronique au terminal, dans la table de conversion. Le terminal mémorise cette table dans une mémoire non volatile.

Selon le premier mode de réalisation, la table de conversion a donc la forme suivante, la devise de référence choisie étant l'euro :

Devise	Taux/euro	Date	Signature
F	0,151	Dat1	SGN(F,0,151,Dat1)
£	1,51	Dat2	SGN(£,1,51,Dat2)
DM	0,50	Dat3	SGN(DM,0,50,Dat3)
L	0,00051	Dat2	SGN(L,0,00051,Dat2)

où F, £, DM, L sont les identifiants désignant respectivement le franc français, la livre britannique, le Mark allemand et la lire italienne, Dat1, Dat2, Dat3 sont des dates de mise à jour des valeurs de taux de conversion et SGN désigne les signatures électroniques calculées par l'autorité bancaire à partir de la valeur de taux de conversion de chaque devise et de sa date de mise à jour.

Selon un deuxième mode de réalisation, la table de conversion peut prendre une forme facilitant le passage d'une devise dans une autre, sans avoir recours à une devise de référence. Cette table contient la valeur de taux de conversion de chaque devise dans toutes les autres devises et a donc la forme suivante :

	euro	F	£	DM	L
euro	1	0,151	1,51	0,50	0,00051
F	6,613	1	9,99	3,345	0,0034
£	6,662	0,1	1	0,334	0,0003
DM	1,976	0,298	2,986	1	0,0005
L	1945	294,1	2938	983,8	1

De même que pour la table précédente, les données sont signées et datées. Pour limiter le nombre de données transmises, l'autorité bancaire transmet au terminal une seule signature, qui peut être calculée à partir de l'ensemble des données contenues dans la table ou à partir d'une combinaison des signatures relatives aux différentes valeurs de taux, et une seule date. Cette combinaison de signatures peut être comprise comme le calcul d'une signature globale à partir des signatures relatives à chaque taux et de la clé et de l'algorithme de signature utilisés.

Les données contenues dans la table de conversion sont certifiées par l'intermédiaire d'une procédure d'authentification connue en soi. Par exemple, l'autorité bancaire calcule une signature électronique d'origine des données à l'aide d'une clé secrète.

Il peut être prévu dans le terminal un module de sécurité pour mémoriser la clé secrète. Un tel module de sécurité renforce la sécurité du système et permet d'augmenter la vitesse des échanges de données, car il

épargne au système un grand nombre de communications entre les cartes et l'autorité bancaire.

La figure 5B illustre un terminal 22 doté d'un module de sécurité 24. Le terminal 22 comprend un microprocesseur 30 auquel sont reliés une mémoire ROM 26, une mémoire RAM 28 et une interface de transmission 32 permettant au terminal de communiquer avec une autorité bancaire. Tous ces éléments sont reliés au module de sécurité 24. Le module de sécurité a la structure électronique de la carte de la figure 1.

Le terminal 22 peut en outre être équipé d'un ou plusieurs modules de stockage tels que des disquettes ou disques amovibles ou non, d'un ou plusieurs modules de saisie (tels qu'un clavier et/ou un dispositif de pointage du type souris) et d'un module d'affichage, ces différents modules n'étant pas représentés sur la figure 5B.

Le terminal peut être constitué par tout appareil informatique installé sur un site privé ou public et apte à fournir des moyens de gestion de l'information ou de délivrance de divers biens ou services, cet appareil étant installé à demeure ou portable. Il peut notamment s'agir d'un appareil dédié aux télécommunications.

Dans le cas où le terminal destinataire de la table de conversion est doté d'un module de sécurité, ce terminal calcule une signature électronique de contrôle avec la même clé secrète que celle qui a servi à l'autorité bancaire pour calculer la signature électronique d'origine, et vérifie que la signature de contrôle est égale à la signature d'origine. Si c'est le cas, l'authenticité des données est vérifiée.

On a vu qu'à chaque valeur de taux de conversion est associée une date de mise à jour. En effet, des mises à jour régulières des valeurs des taux de conversion sont effectuées, par exemple une fois par jour, par une

communication entre le terminal et l'autorité bancaire. Le terminal écrit dans une mémoire non volatile les données de conversion et la signature de l'autorité bancaire.

On donne ci-après un exemple concret d'utilisation de la carte. Un porteur d'une carte PME contenant 100 francs se rend en Allemagne et souhaite effectuer un achat d'un produit d'une valeur de 20 DM.

Le porteur introduit sa carte dans le terminal bancaire. Le terminal interroge le solde de la carte et constate qu'il est en francs, en lisant l'identifiant de la devise. Le terminal demande alors à la carte de convertir son solde en Marks. Pour cela, le terminal transmet à la carte la table de conversion qu'il possède en mémoire, ou une partie de cette table, incluant la ou les date(s) de mise à jour et la ou les signature(s) électronique(s) d'origine, selon que la table de conversion est conforme au premier ou au deuxième mode de réalisation décrits ci-dessus.

Une fois les données reçues, la carte vérifie leur authenticité en calculant une ou des signature(s) de contrôle avec la clé secrète de l'autorité bancaire, selon un protocole de communication décrit en détail plus loin. Si les signatures d'origine et de contrôle ne sont pas égales, la conversion n'est pas effectuée et la carte en informe le terminal, qui le signale au porteur sous forme d'un message d'erreur.

Si les signatures sont égales, et à supposer que la table soit conforme au deuxième mode de réalisation, la carte recherche dans la table de conversion la valeur située au croisement de la colonne correspondant à la devise de départ et de la ligne correspondant à la devise courante.

Dans l'exemple, la valeur permettant de convertir des francs en Marks est 0,298. Puis la carte multiplie son



15

solde actuel par la valeur du taux et obtient le nouveau solde en Marks : 29,8 DM. Cette nouvelle valeur est inscrite dans la mémoire non volatile de la carte et elle est envoyée au terminal. Celui-ci vérifie que le nouveau solde est suffisant pour effectuer la transaction, ce qui est le cas dans l'exemple. La transaction est donc menée à bien.

Dans le cas où la table de conversion utilisée est conforme au premier mode de réalisation ci-dessus, la conversion effectuée par la carte consiste d'abord à multiplier le solde en francs par la valeur du taux de conversion des francs en euros, soit 0,151. Puis la valeur obtenue est multipliée par l'inverse de la valeur du taux de conversion des Marks en euros, soit 1/0,50.

On va maintenant décrire de façon générale le protocole de communication entre la carte et le terminal, en référence aux figures 5A et 5C.

Dans le cas illustré par la figure 5A, où le terminal ne dispose pas d'un module de sécurité, le terminal reçoit tout d'abord une table de conversion en provenance d'une autorité bancaire, accompagnée d'une signature électronique d'origine  $S_K$  relative au taux de conversion de la devise de départ dans la devise courante, cette signature  $S_K$  ayant été établie par l'autorité bancaire à partir de la valeur de taux de conversion et au moyen d'un algorithme cryptographique déterminé tel que RSA ou DES, et au moyen d'une clé secrète  $K$ .

Lorsqu'on introduit la carte dans le terminal, la table de conversion et la signature électronique d'origine  $S_K$  sont transmises à la carte en provenance de l'autorité bancaire, le terminal ayant ici une simple fonction de mémoire tampon.

Dans le cas où la table de conversion utilisée est du type décrit dans le premier mode de réalisation ci-

dessus, l'autorité bancaire peut transmettre à la carte uniquement les lignes de la table de conversion correspondant aux valeurs de taux de conversion des devises de départ et courante concernées par la conversion.

5 Dans le cas illustré par la figure 5C, où le terminal dispose d'un module de sécurité, le terminal commence par recevoir, en provenance de l'autorité bancaire, une table de conversion. Il a préalablement  
10 mémorisé une clé K ainsi qu'un algorithme cryptographique, par exemple du type RSA ou DES, fournis par cette autorité bancaire, qui vont lui servir à authentifier la table de conversion reçue : le terminal va par exemple recalculer la signature et la comparer avec celle reçue de l'autorité. Avantageusement, la clé K est une clé secrète et est  
15 mémorisée dans le module de sécurité du terminal 24 illustré par la figure 5B.

Lorsqu'on introduit la carte dans le terminal, afin de réaliser une transaction dans une devise courante alors que la carte utilise habituellement une devise de départ  
20 différente de la devise courante et si l'authenticité de la table de conversion est confirmée, le terminal transmet à la carte le taux de conversion de la devise de départ dans la devise courante, contenu dans la table de conversion. Le terminal transmet simultanément à la carte la signature  
25 électronique d'origine  $S_K$  relative à ce taux.

La signature électronique d'origine  $S_K$  relative au taux de conversion est calculée à partir d'un certain nombre de données. La signature  $S_K$  peut par exemple être  
30 calculée à partir de la valeur de taux de conversion et de la date d'élaboration de ce taux. Pour plus de sécurité, la signature  $S_K$  peut être calculée, non seulement à partir de ces données, mais en outre à partir d'un numéro d'identification spécifique à la carte, mémorisé dans la partie système de la mémoire programmable non volatile de

la carte, éventuellement complétée par une valeur aléatoire fournie par la carte.

Dans les deux cas illustrés par les figures 5A et 5C, l'étape suivante du protocole de communication entre la carte et le terminal consiste, pour la carte, à calculer une signature électronique de contrôle  $S_{KC}$  relative à la valeur de taux de conversion reçue du terminal ou de l'autorité bancaire, à l'aide d'une clé et d'un algorithme cryptographique préalablement mémorisés dans la carte.

La carte compare ensuite la signature de contrôle  $S_{KC}$  qu'elle a calculée et la signature d'origine  $S_K$  qu'elle a reçue du terminal ou de l'autorité bancaire. Si ces deux signatures sont identiques, la carte effectue la conversion de son solde courant mémorisé de la devise de départ dans la devise courante au moyen du taux de conversion reçu et mémorise le solde courant converti, puis effectue la transaction prévue. Si les deux signatures diffèrent, toute possibilité de conversion est bloquée et un message d'erreur est émis.

Dans ce qui précède, on a décrit un procédé de vérification de signature consistant à recalculer la signature à partir d'un message constitué par le taux de conversion et la date d'élaboration de ce taux, et à la comparer à la signature reçue. En variante, on peut naturellement partir de la signature reçue et vérifier qu'elle provient bien du message précité, par exemple en utilisant un algorithme inverse de celui utilisé pour calculer la signature, lorsque cet algorithme existe. Si cette variante utilise un algorithme dissymétrique, ladite vérification utilisera une clé publique corrélée à une clé secrète ayant servi à calculer la signature.

Comme indiqué plus haut, en référence à la figure 4, la mémoire programmable non volatile de la carte mémorise les transactions, dans une mémoire dite de trace.

A titre d'exemple non limitatif, cette mémoire de trace peut être organisée en blocs de données et gérée de façon cyclique. Dans ce cas, tous les blocs sont rangés séquentiellement. Dès que la mémoire de trace est pleine, la transaction suivante est inscrite à l'emplacement de la transaction la plus ancienne.

Chaque bloc de données de la mémoire de trace comprend les éléments suivants :

- Type de transaction : débit, crédit ou conversion
- Date de la transaction
- Montant de la transaction
- Solde de la carte
- Devise utilisée pour exprimer le solde de la carte et le montant de la transaction

En option, le bloc de données peut également comprendre les éléments suivants :

- Identifiant du terminal et/ou du module de sécurité du terminal
- Valeur du taux de conversion
- Date d'élaboration du taux par l'autorité bancaire
- Référence de l'autorité bancaire qui a émis la valeur du taux

Ces éléments optionnels peuvent être utilisés pour réaliser un contrôle des opérations effectuées par la carte. En cas de contestation du porteur, elles permettent une expertise de la carte.

Un mode particulier de réalisation du protocole de communication entre la carte PME et le terminal permet de limiter le risque de création frauduleuse de monnaie. Une telle fraude consiste à avoir recours successivement à plusieurs terminaux disposant de tables de conversion

élaborées à des dates différentes, les valeurs des taux de conversion ayant fluctué entre ces différentes dates.

Par exemple, supposons qu'un fraudeur dispose de deux terminaux. Le premier possède en mémoire une table de conversion dans laquelle le taux de conversion entre le franc et le Mark est le suivant :  $DM = 0,4 \times F$ , ce qui équivaut à  $F = 2,5 \times DM$ , où  $F$  désigne le franc et  $DM$  désigne le Mark. Le second terminal possède une table de conversion dans laquelle le taux correspondant est :

$$F = 3 \times DM, \text{ ou } DM = 0,33 \times F.$$

Si le fraudeur introduit une carte PME ayant un solde courant  $S1$  en francs dans le premier terminal pour effectuer une conversion, la carte calcule le solde  $S2$  en Marks suivant la formule :  $S2 = 0,4 \times S1$ . puis le fraudeur introduit sa carte dans le second terminal pour effectuer la conversion inverse et obtenir un solde  $S3$  en francs :

$$S3 = 3 \times S2 = 3 \times 0,4 \times S1 = 1,2 \times S1.$$

Il y a donc eu création illégale de monnaie et enrichissement sans cause.

Pour empêcher une telle fraude, la carte effectue une vérification supplémentaire, illustrée par la figure 8, lorsqu'elle reçoit la table de conversion. Elle vérifie que la date  $D_1$  d'élaboration de la table de conversion reçue est postérieure à la date  $D_2$  de la dernière transaction qu'elle a mémorisée dans sa mémoire de trace.

Les dates  $D_1$  et  $D_2$  sont initialement exprimées en année, mois, jour, heures, minutes, secondes. La carte convertit  $D_1$  et  $D_2$  en valeurs numériques, puis compare les deux valeurs numériques obtenues. Si  $D_1 > D_2$ , la vérification est positive et la transaction se poursuit. Dans le cas contraire, c'est-à-dire si la fraude est avérée, il y a blocage total de la carte, qui ne peut être éventuellement débloquée que par une clé spécifique de déblocage.

Cette vérification supplémentaire permet d'éviter l'utilisation d'une table de conversion qui n'a plus cours. De plus, pour éviter de rechercher la date de la dernière transaction dans la mémoire de trace, la date et le taux de conversion peuvent être inscrits dans la partie système de la mémoire programmable non volatile de la carte.

Un autre type de fraude, contre lequel la présente invention propose deux parades, consiste à disposer d'un nombre important de terminaux, disposant tous de tables de conversion authentiques et mises à jour à des dates différentes et connues du fraudeur. Si le fraudeur introduit successivement une carte PME dans les terminaux de façon à respecter la chronologie des dates de mise à jour, pour peu que les valeurs des taux de conversion aient beaucoup fluctué dans l'intervalle de temps entre la première et la dernière mises à jour, le fraudeur pourra augmenter le solde de sa carte.

Une première parade à ce type de fraude consiste à doter le module de sécurité du terminal d'un compteur de conversions  $CO_i$ , où  $i$  est l'indice de la conversion actuelle, comme le montre la figure 6. Le compteur  $CO_i$  est incrémenté à chaque demande de conversion. Lorsque le compteur atteint une valeur maximale  $M$  prédéterminée,  $M=100$  par exemple, le terminal inhibe toute possibilité de transaction et se met en communication avec l'autorité bancaire afin de recevoir une table de conversion mise à jour. Une fois cette nouvelle table reçue, le compteur est remis à zéro.

Plus précisément, le module de sécurité du terminal mémorise une table de conversion et le compteur est incrémenté chaque fois que le terminal demande à son module de sécurité de lui fournir un taux authentifié. Si le compteur atteint sa valeur maximale, le module ne fournit plus d'information.

Une seconde parade à ce type de fraude consiste à doter le terminal d'une horloge ou d'un moyen quelconque permettant de recevoir la date et l'heure. Comme le montre la figure 7, il peut s'agir par exemple d'un récepteur radio intégré au terminal ou à la carte, qui reçoit les signaux de date et heure  $D_R$  émis par l'Observatoire de Brunswick. Si l'écart  $\delta = D_R - D_E$  entre la date  $D_E$  de mise à jour de la table et la date  $D_R$  de l'horloge interne dépasse une certaine durée, par exemple une heure, le terminal se bloque car la tentative de fraude est avérée et, de même que dans le cas de la première parade, n'effectue plus aucune transaction tant qu'une table de conversion plus récente n'a pas été chargée. Seule une procédure spécifique permet alors de débloquer le terminal.

## REVENDICATIONS

1. Dans un objet portatif (10) comportant au moins une application de porte-monnaie électronique, cet objet portatif comprenant des moyens de traitement de l'information (14) et au moins une mémoire programmable non volatile (18), comportant une zone de mémorisation de transactions relatives à l'application de porte-monnaie électronique, ces transactions comportant au moins une instruction d'opération de débit et une instruction d'opération de crédit, un protocole d'échange de données définissant une instruction d'opération de conversion de monnaie électronique d'une devise de départ en une devise courante, consistant au moins à :

(a) mémoriser dans ledit objet portatif (10) une table de conversion de monnaie électronique certifiée par au moins une signature électronique d'origine ( $S_K$ ) par une autorité bancaire, ladite table de conversion de monnaie électronique comportant au moins une valeur de taux de conversion d'une devise de départ en au moins une devise courante ;

(b) authentifier ladite table de conversion de monnaie électronique, par vérification de ladite signature électronique d'origine ( $S_K$ ), et, en cas d'authentification de ladite table de conversion de monnaie électronique, la valeur de taux de conversion constituant une valeur de taux de conversion authentifiée,

(c) procéder à la conversion d'un solde courant du porte-monnaie électronique, à partir de ladite valeur de taux de conversion authentifiée, pour engendrer une valeur du



solde courant convertie, et mémoriser la valeur du solde courant convertie dans ladite mémoire non volatile, ou, en l'absence d'authentification,

5 (d) bloquer une transaction courante.

2. Protocole selon la revendication 1, suivant lequel ladite table de conversion de monnaie électronique contient, pour plusieurs devises prédéterminées,

- un identifiant désignant chacune de ces devises,
- 10 - une valeur de taux de conversion de chacune de ces devises dans une devise de référence commune,
- une date de mise à jour de chacune desdites valeurs de taux de conversion, et
- une signature associée à chacune desdites valeurs de
- 15 taux de conversion, calculée à partir dudit identifiant, de ladite valeur de taux de conversion et de ladite date, au moyen d'un algorithme prédéterminé.

3. Protocole selon la revendication 1, suivant lequel ladite table de conversion de monnaie électronique contient, pour plusieurs devises prédéterminées,

- 20 - un identifiant désignant chacune de ces devises,
- une valeur de taux de conversion de chacune de ces devises dans toutes les autres devises,
- une date de mise à jour de ladite table, et
- 25 - une signature calculée à partir de l'ensemble des données contenues dans la table, au moyen d'un algorithme prédéterminé.

4. Protocole selon la revendication 1, suivant lequel l'objet portatif (10) comprend en outre

- 30 - des moyens de comparaison entre une date de mise à jour associée à une nouvelle valeur de taux de conversion reçue et une date associée à une ancienne valeur de taux de conversion mémorisée, et

- une clé délivrée par l'autorité bancaire, associée à un algorithme de vérification de signature électronique prédéterminé.

5           5.       Protocole selon la revendication 1, suivant lequel ladite mémoire programmable non volatile comprend au moins une mémoire du type EPROM, EEPROM ou FERAM.

10           6.       Protocole selon la revendication 1, suivant lequel ladite zone de mémorisation de transactions est du type cyclique à N emplacements, pour mémoriser N transactions, la (N+1)<sup>ème</sup> transaction étant mémorisée à l'emplacement de la première transaction et provoquant l'effacement de ladite première transaction.

15           7.       Protocole de communication entre un objet portatif (10) utilisant une première devise habituelle prédéterminée et un terminal de transaction utilisant une deuxième devise habituelle prédéterminée, ledit objet portatif (10) comportant au moins une application de porte-monnaie électronique, et comprenant des moyens de traitement de l'information (14) et au moins une mémoire programmable non volatile (18) comportant une zone de mémorisation de transactions relatives à l'application de porte-monnaie électronique, ces transactions comportant au moins une instruction d'opération de débit et une instruction d'opération de crédit, ledit protocole de communication comprenant des étapes suivant lesquelles :

- 25           (a)       le terminal reçoit en provenance d'une autorité bancaire une table de conversion de monnaie électronique ;
- 30           (b)       on introduit dans le terminal ledit objet portatif afin de réaliser une transaction ;
- (c)       le terminal transmet à l'objet portatif le taux de conversion de ladite première devise dans ladite deuxième devise, contenu dans ladite table de conversion de monnaie

électronique, accompagné d'une signature électronique d'origine ( $S_K$ ) relative audit taux, ladite signature électronique d'origine ( $S_K$ ) étant calculée à l'aide d'une

(d) l'objet portatif vérifie ladite signature électronique d'origine ( $S_K$ ) à l'aide de ladite clé, préalablement mémorisée dans l'objet portatif ou d'une clé corrélée à celle-ci ;

(e) si la signature électronique d'origine ( $S_K$ ) est vérifiée, l'objet portatif effectue la conversion du solde courant mémorisé de ladite première devise dans ladite deuxième devise au moyen dudit taux de conversion et mémorise le solde courant converti ;

(f) l'objet portatif effectue ladite transaction.

8. Protocole de communication selon la revendication 7, suivant lequel, à l'issue de l'étape (a), le terminal vérifie l'authenticité de ladite table de conversion de monnaie électronique à l'aide d'une clé fournie par l'autorité bancaire.

9. Protocole de communication selon la revendication 8, suivant lequel, à l'issue de l'étape (a), le terminal compare en outre la date d'élaboration ( $D_E$ ) de ladite table de conversion de monnaie électronique à une date courante de référence ( $D_R$ ) reçue par voie hertzienne, et si l'écart ( $\delta$ ) entre ces dates dépasse un seuil prédéterminé, le terminal inhibe toute possibilité de transaction et se met en communication avec l'autorité bancaire afin de recevoir une table de conversion de monnaie électronique mise à jour.

10. Protocole de communication selon la revendication 7, suivant lequel ladite signature électronique d'origine ( $S_K$ ) est calculée à partir de la date d'élaboration dudit taux de conversion.

5 11. Protocole de communication selon la revendication 7, suivant lequel ladite clé est une clé secrète mémorisée dans un module de sécurité dudit terminal.

10 12. Protocole de communication selon la revendication 7, suivant lequel, à l'étape (d), l'objet portatif compare la date ( $D_1$ ) d'élaboration du taux de conversion reçu à la date ( $D_2$ ) de la dernière transaction mémorisée et vérifie que la date ( $D_1$ ) d'élaboration du taux de conversion reçu est postérieure à la date ( $D_2$ ) de la  
15 dernière transaction mémorisée.

13. Protocole de communication selon la revendication 7, suivant lequel, à l'issue de l'étape (e), le terminal incrémente un compteur de conversions, et lorsque ledit compteur atteint une valeur maximale  
20 prédéterminée, le terminal inhibe toute possibilité de transaction et se met en communication avec l'autorité bancaire afin de recevoir une table de conversion mise à jour.

25 14. Protocole de communication selon la revendication 13, suivant lequel ledit compteur est compris dans un module de sécurité dudit terminal.

30 15. Protocole de communication selon la revendication 7, suivant lequel, à l'étape (c), ladite signature électronique d'origine est calculée à partir d'un paramètre supplémentaire consistant en un numéro d'identification de l'objet portatif introduit et/ou une valeur aléatoire fournie par ledit objet portatif.

16. Objet portatif comprenant des moyens de traitement de l'information (14) et des moyens de

mémorisation de l'information(18), caractérisé en ce qu'il inclut :

- 5 - des moyens pour stocker de façon provisoire dans les moyens de mémorisation une table de conversion de monnaie électronique reçue de l'extérieur de l'objet portatif et comportant au moins une valeur de taux de conversion d'une devise de départ en au moins une devise courante, ainsi qu'une signature électronique d'origine ( $S_K$ ) de cette table de conversion, calculée au moyen  
10 d'un algorithme de signature et d'une clé de signature déterminés ;
- des moyens pour authentifier ladite table de conversion en vérifiant ladite signature électronique d'origine ( $S_K$ ) de la table de conversion reçue, au moyen d'un  
15 algorithme de vérification de signature et d'une clé de vérification de signature déterminés ;
- des moyens pour stocker de façon durable, en cas d'authentification positive, la table de conversion dans les moyens de mémorisation ; et
- 20 - des moyens pour calculer une valeur de solde courant convertie à partir d'une valeur de solde courant et d'une valeur de taux de conversion extraite de la table de conversion authentifiée.

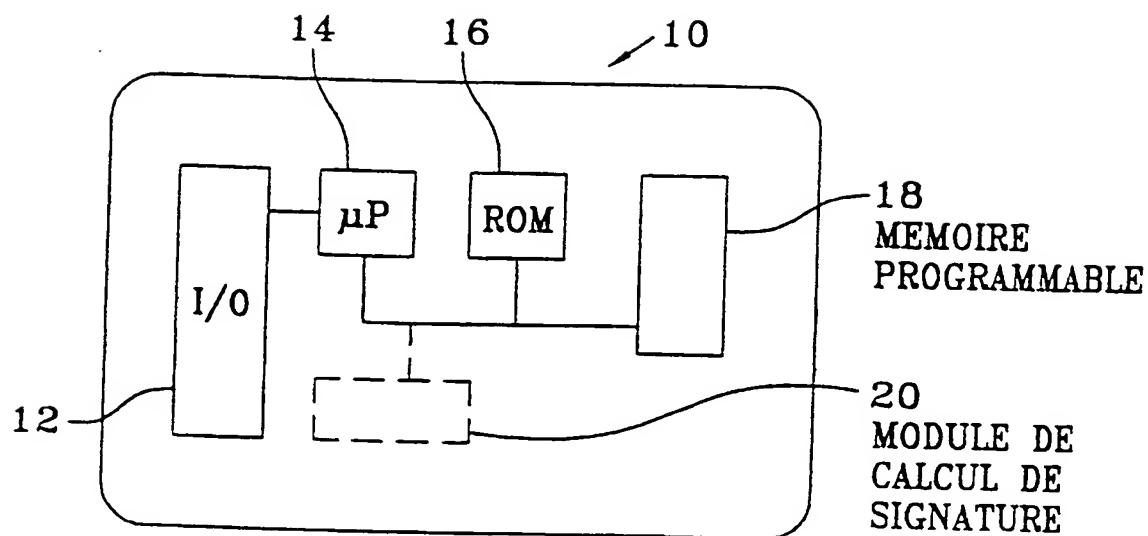


FIG.1

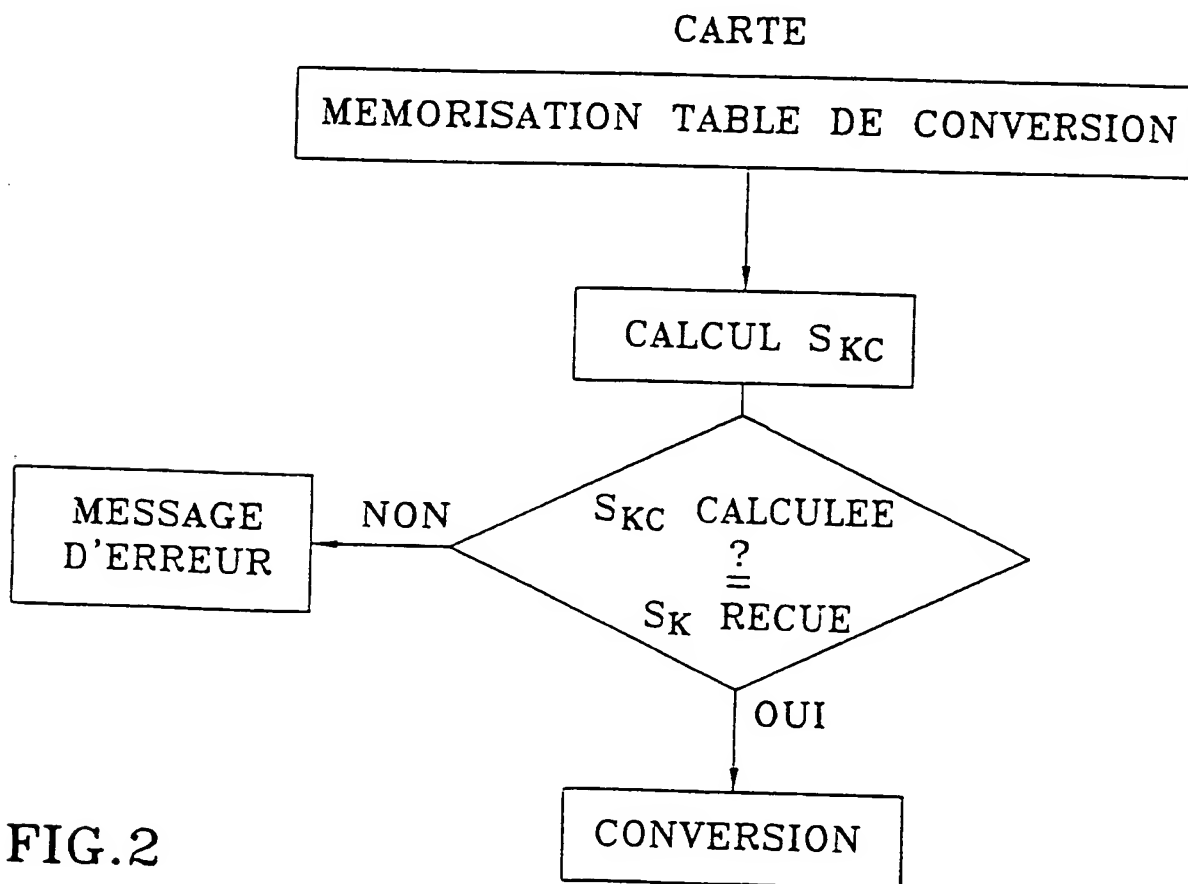


FIG.2

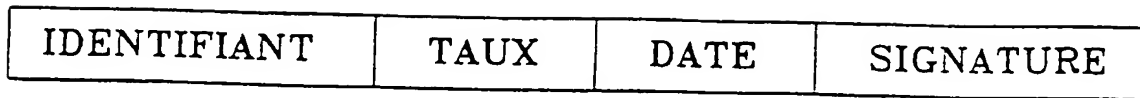


FIG.3

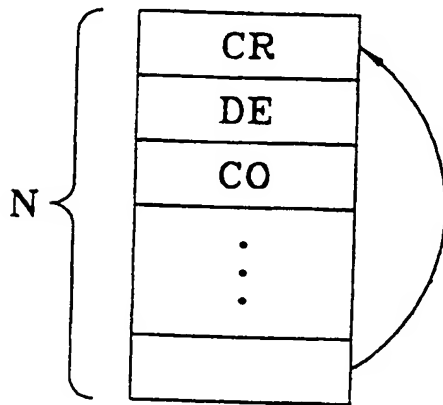


FIG.4

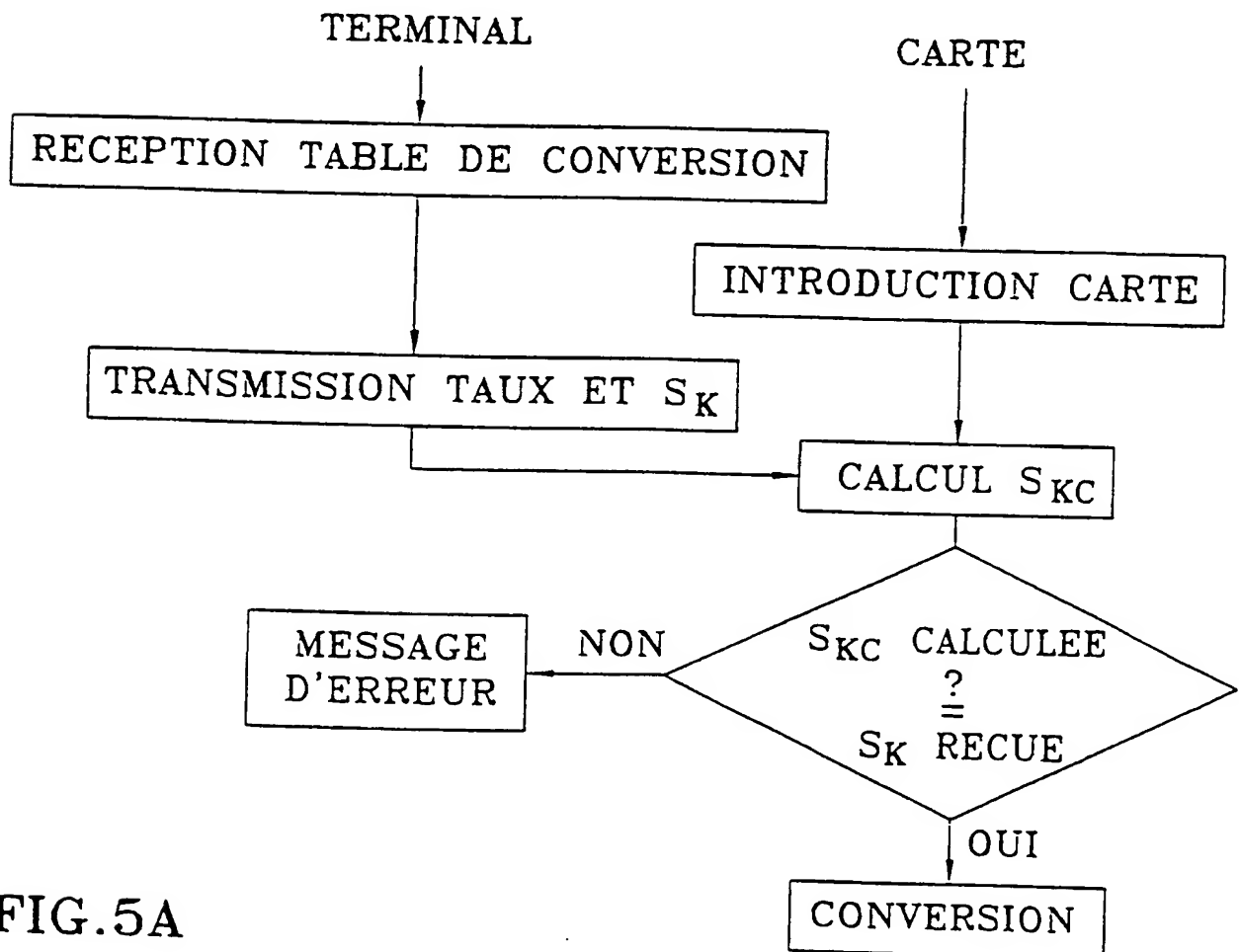


FIG.5A

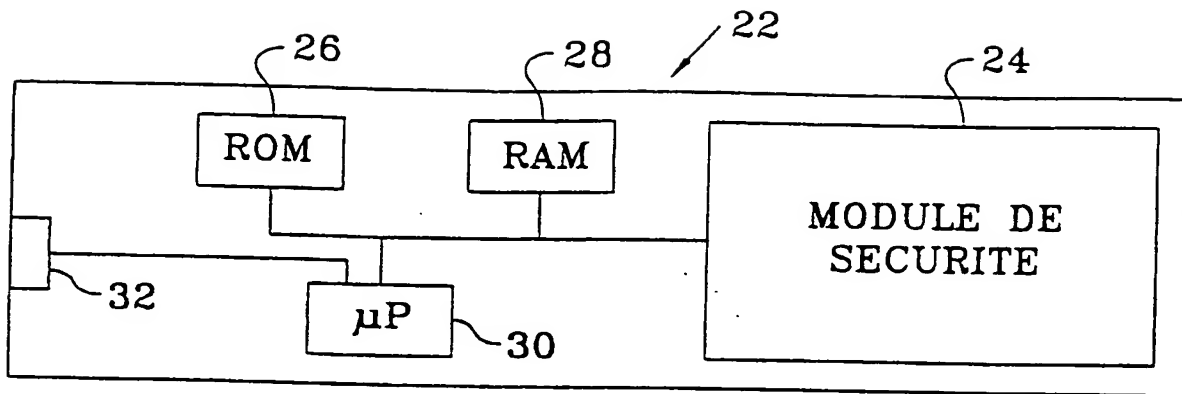


FIG.5B

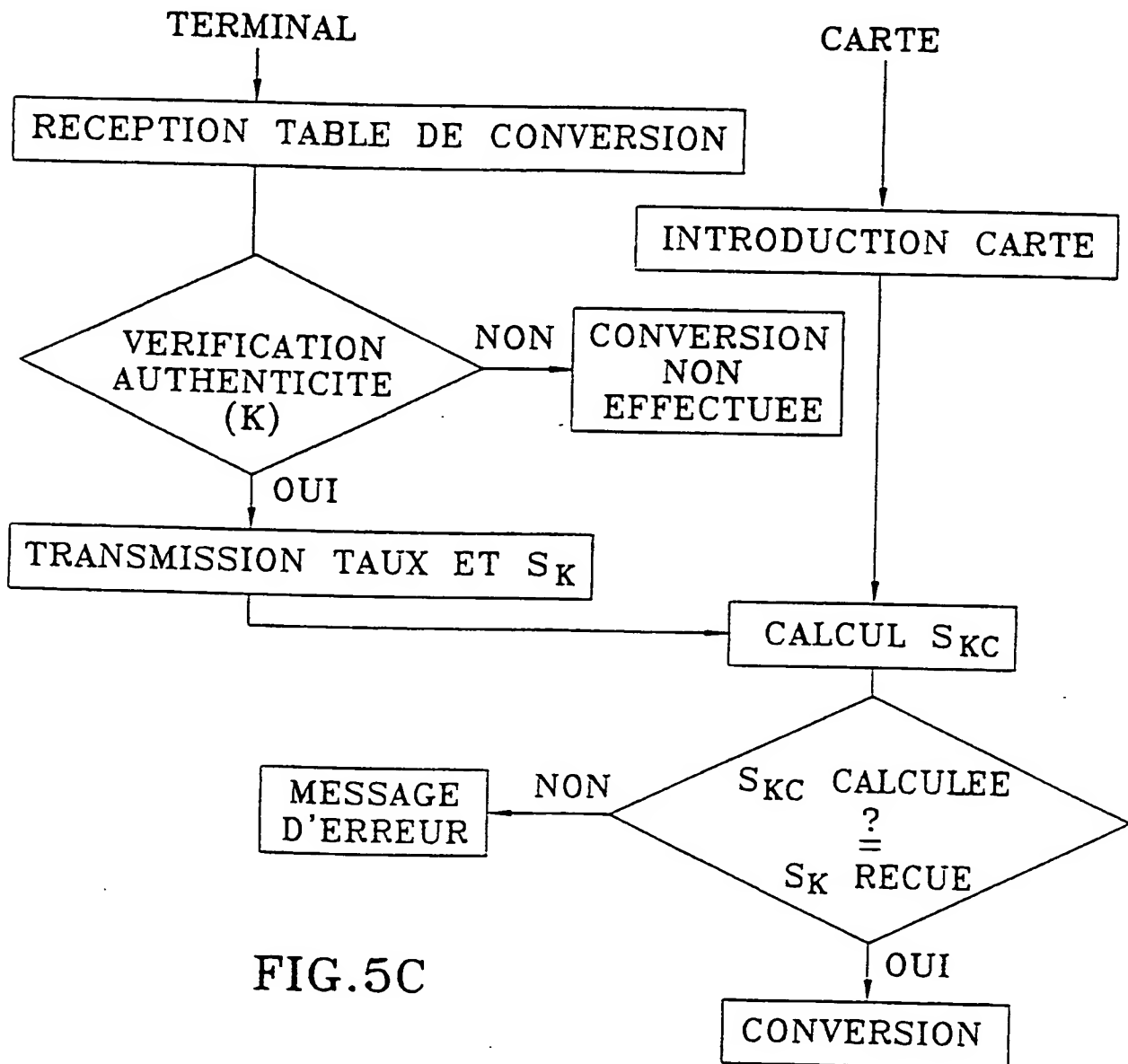


FIG.5C



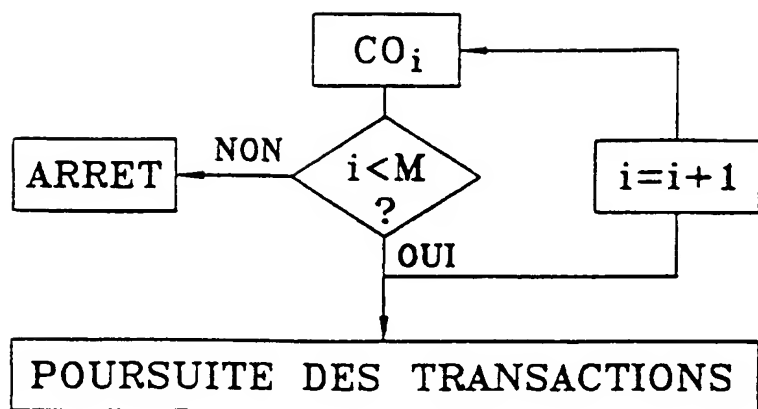


FIG.6

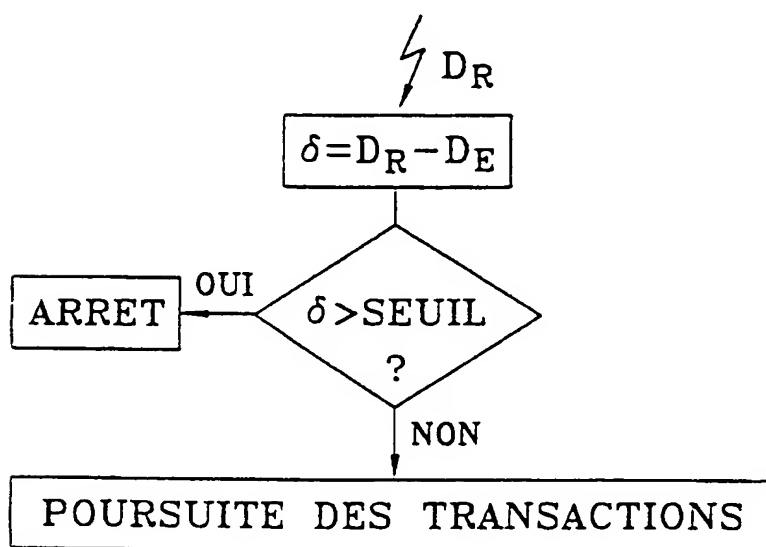


FIG.7

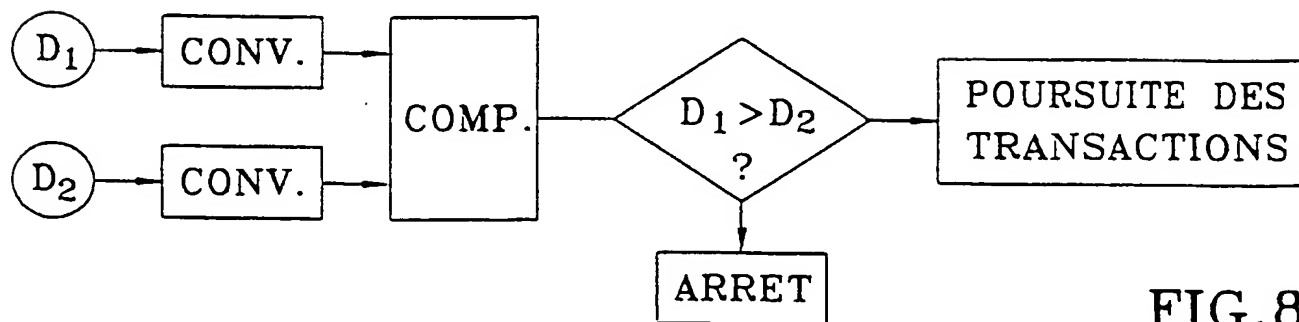


FIG.8

# INTERNATIONAL SEARCH REPORT

National Application No  
PCT/FR 99/02014

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 36024 A (NEDERLAND PTT) 14 November 1996 (1996-11-14) abstract; figures 1-3 page 3, line 8 -page 5, line 9 page 5, line 21 -page 9, line 6 ----	1-3, 7, 8, 16
A	WO 93 08545 A (JONHIG LTD) 29 April 1993 (1993-04-29) abstract; figure 1 page 3, line 17 -page 7, line 9 page 10, line 20 -page 11, line 7 ----	1, 7, 16
A	US 4 968 873 A (HINNEBERG CHRISTIAN ET AL) 6 November 1990 (1990-11-06) abstract; figures 1,11-13 column 7, line 46 - line 61 column 14, line 37 -column 15, line 63 ----- -/-	1, 7, 16

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier document but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.  
"&" document member of the same patent family

Date of the actual completion of the international search

28 October 1999

Date of mailing of the international search report

05/11/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Authorized officer

Buron, E

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/FR 99/02014

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 750 283 A (OKI ELECTRIC IND CO LTD) 27 December 1996 (1996-12-27) abstract; figure 1 column 2, line 29 -column 3, line 53 column 31, line 38 -column 32, line 3 -----	1,7,16
A	EP 0 251 619 A (VISA INT SERVICE ASS) 7 January 1988 (1988-01-07) abstract; figures 1-3 page 4, line 8 -page 6, line 16 page 7, line 1 -page 8, line 20 page 9, last paragraph -page 13, paragraph 1 -----	1,16

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 99/02014

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9636024	A	14-11-1996	NL 1000352 C AU 701801 B AU 5816196 A CA 2220748 A EP 0824741 A NO 975157 A	13-11-1996 04-02-1999 29-11-1996 14-11-1996 25-02-1998 08-01-1998
WO 9308545	A	29-04-1993	AT 145744 T AU 663739 B AU 2888692 A BR 9205416 A CA 2098481 A DE 69215501 D DE 69215501 T DK 567610 T EP 0567610 A ES 2096772 T GR 3022528 T HK 1001573 A JP 2853331 B JP 6503913 T NO 303893 B PL 299825 A US 5440634 A	15-12-1996 19-10-1995 21-05-1993 17-05-1994 17-04-1993 09-01-1997 27-03-1997 17-02-1997 03-11-1993 16-03-1997 31-05-1997 26-06-1998 03-02-1999 28-04-1994 14-09-1998 18-04-1994 08-08-1995
US 4968873	A	06-11-1990	US 4837422 A CN 1031902 A, B DD 282308 A DD 282306 A DE 3867001 A EP 0306892 A JP 1145798 A JP 2597672 B RU 2060540 C	06-06-1989 22-03-1989 05-09-1990 05-09-1990 30-01-1992 15-03-1989 07-06-1989 09-04-1997 20-05-1996
EP 0750283	A	27-12-1996	NO 963725 A US 5854581 A WO 9524690 A JP 2828344 B	06-09-1996 29-12-1998 14-09-1995 25-11-1998
EP 0251619	A	07-01-1988	US 4766293 A AT 80484 T AU 587756 B AU 7255987 A CA 1270326 A DE 3781606 A JP 2072954 C JP 7089358 B JP 63257089 A	23-08-1988 15-09-1992 24-08-1989 07-01-1988 12-06-1990 15-10-1992 25-07-1996 27-09-1995 24-10-1988

# RAPPORT DE RECHERCHE INTERNATIONALE

Recherche Internationale No  
PCT/FR 99/02014

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)  
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 96 36024 A (NEDERLAND PTT) 14 novembre 1996 (1996-11-14) abrégé; figures 1-3 page 3, ligne 8 -page 5, ligne 9 page 5, ligne 21 -page 9, ligne 6 ---	1-3,7,8, 16
A	WO 93 08545 A (JONHIG LTD) 29 avril 1993 (1993-04-29) abrégé; figure 1 page 3, ligne 17 -page 7, ligne 9 page 10, ligne 20 -page 11, ligne 7 ---	1,7,16
A	US 4 968 873 A (HINNEBERG CHRISTIAN ET AL) 6 novembre 1990 (1990-11-06) abrégé; figures 1,11-13 colonne 7, ligne 46 - ligne 61 colonne 14, ligne 37 -colonne 15, ligne 63 --- -/--	1,7,16

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

**Catégories spéciales de documents cités:**

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

28 octobre 1999

Date d'expédition du présent rapport de recherche internationale

05/11/1999

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Buron, E

# RAPPORT DE RECHERCHE INTERNATIONALE

Recherche Internationale No

PCT/FR 99/02014

## C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 750 283 A (OKI ELECTRIC IND CO LTD) 27 décembre 1996 (1996-12-27) abrégé; figure 1 colonne 2, ligne 29 -colonne 3, ligne 53 colonne 31, ligne 38 -colonne 32, ligne 3 ---	1,7,16
A	EP 0 251 619 A (VISA INT SERVICE ASS) 7 janvier 1988 (1988-01-07) abrégé; figures 1-3 page 4, ligne 8 -page 6, ligne 16 page 7, ligne 1 -page 8, ligne 20 page 9, dernier alinéa -page 13, alinéa 1 -----	1,16

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Requête internationale No

PCT/FR 99/02014

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9636024	A	14-11-1996	NL 1000352 C	13-11-1996
			AU 701801 B	04-02-1999
			AU 5816196 A	29-11-1996
			CA 2220748 A	14-11-1996
			EP 0824741 A	25-02-1998
			NO 975157 A	08-01-1998
WO 9308545	A	29-04-1993	AT 145744 T	15-12-1996
			AU 663739 B	19-10-1995
			AU 2888692 A	21-05-1993
			BR 9205416 A	17-05-1994
			CA 2098481 A	17-04-1993
			DE 69215501 D	09-01-1997
			DE 69215501 T	27-03-1997
			DK 567610 T	17-02-1997
			EP 0567610 A	03-11-1993
			ES 2096772 T	16-03-1997
			GR 3022528 T	31-05-1997
			HK 1001573 A	26-06-1998
			JP 2853331 B	03-02-1999
			JP 6503913 T	28-04-1994
			NO 303893 B	14-09-1998
			PL 299825 A	18-04-1994
			US 5440634 A	08-08-1995
US 4968873	A	06-11-1990	US 4837422 A	06-06-1989
			CN 1031902 A, B	22-03-1989
			DD 282308 A	05-09-1990
			DD 282306 A	05-09-1990
			DE 3867001 A	30-01-1992
			EP 0306892 A	15-03-1989
			JP 1145798 A	07-06-1989
			JP 2597672 B	09-04-1997
			RU 2060540 C	20-05-1996
EP 0750283	A	27-12-1996	NO 963725 A	06-09-1996
			US 5854581 A	29-12-1998
			WO 9524690 A	14-09-1995
			JP 2828344 B	25-11-1998
EP 0251619	A	07-01-1988	US 4766293 A	23-08-1988
			AT 80484 T	15-09-1992
			AU 587756 B	24-08-1989
			AU 7255987 A	07-01-1988
			CA 1270326 A	12-06-1990
			DE 3781606 A	15-10-1992
			JP 2072954 C	25-07-1996
			JP 7089358 B	27-09-1995
			JP 63257089 A	24-10-1988

**THIS PAGE BLANK (USPTO)**